REMARKS

Claims 1-51 are pending in the present application. In the above amendments, claims 1-7, 11-20, 22-29, 33, and 35-51 have been amended to clarify the claimed subject matter. No new claims have been added.

Applicant respectfully responds to this Office Action.

Specification

The Office Action objected to paragraphs 11 and 12 as since the private and public keys are misused. Applicant has amended paragraphs 11 and 12 to clarify the specification. Applicant believes that this objection has been addressed.

Additionally, paragraphs 32 and 33 have also been amended to correct typographical errors in the reference numbers.

Claim Rejections – 35 USC § 112

The Office Action rejected claims 2, 7, 14-21, 23 and 36-42 under 35 U.S.C. §112, second paragraph, as being indefinite for being unclear.

With regard to claims 2, 15, and 23, the Office Action alleges that the language "second public key" appears to be misused. Applicant has amended the claims to recite "second private key" instead. Therefore, Applicant submits these rejections have been overcome.

With regard to claim 7, the Office Action alleges that the language is unclear. Applicant has amended claim 7 to clarify its scope.

With regard to claims 14-21 and 36-42, the Office Action alleges that these claims recite apparatus claims but all that is listed is software per se. The form of these claims is consistent with 35 U.S.C. 112, paragraph six. Applicant submits that these are "means-plus-function" claims that cover an apparatus to perform the recited functions. Such apparatus may include, for example, a processor, a storage medium, a transmitter, and/or a receiver illustrated in Figure 1 of the present application. Consequently, Applicant submits that the form of these claims is proper.

Claim Rejections – 35 USC § 101

The Office Action rejected claims 14-21 and 36-42 under 35 U.S.C. §101 because the invention is alleged to be directed to non-statutory subject matter since the claims lack the necessary physical articles or objects to constitute a machine or a manufacture. Applicant again submits that claims 14-21 and 36-42 are "means-plus-function" claims consistent with 35 U.S.C. 112, paragraph six. Consequently, the subject of these claims is statutory.

Applicant believes that the Office Action may have meant to refer to claims 22-28 and 43-49 as being non-statutory. Applicant has clarified the terms of claims 22-28 and 43-49 to more clearly recite a Beauregard claim structure, claiming a public cryptography process stored in a machine-readable medium. Applicant submits that these claims recite proper statutory subject matter.

Claim Rejections – 35 USC § 102

Claims 1, 11, 14, 19, 22, 26, 50 and 51

The Office Action rejected independent claims 1, 11, 14, 19, 22, 26, 50 and 51 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,959,393 to Robert L. Hollis et al. (hereinafter "Hollis").

The rejection is respectfully traversed in its entirety.

The Hollis patent discloses a method for securely and dynamically transporting private or sensitive data over existing non-secure networks without overhead and limited security associated with traditional virtual private network (VPN) solutions. In particular, the system disclosed by Hollis describes how non-secured servers are secured by using public-private key cryptography to protect private data transmissions through the servers (nodes). However, it is clear that Hollis uses the public-private key pairs to encrypt communications between the servers (nodes) thereby providing security to private data transmissions. (See Abstract – "Standard encryption algorithms are used to minimize the threat of eavesdropping.").

The present claims are focused on authentication of subscriber user device (e.g., mobile phones) with a network verifier. To clarify the focus of the present claims 1, 11, 14, 19, 22, 26, 50 and 51 have been amended to recite that the public-private key pairs are generated and sent by a mobile user device (e.g., wireless phone, mobile phone, token, etc.).

To anticipate a claim under 35 U.S.C. § 102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the … claim." (see MPEP §2131).

Applicant submits that Hollis fails to teach a method "operational in a mobile user device for authentication in a public cryptographic system ..." or a verification method/device configured to "receiving a first public key from a mobile user device, means for receiving a second public key from the mobile user device ..." As noted above, Hollis is aimed at securing data communications as it travels across rendezvous points (RVP) (nodes, servers) of a public data network by using a public-private key pair between each node to encrypt communications. (Col. 8, lines 52-54 – "The Public-Private Key paradigm is a proven security methodology for encrypting transmitted information."). The rendezvous points (RVP) do not generate their own public-private key pair but appear to obtain the public-private key pairs from a centralized "key authority" (KA).

By contrast, the present claimed invention is aimed at authenticating mobile user devices with a network verifier. Each mobile user device generates is own public-private key pair (and a backup public-private key pair) and distributes the public key to the verifier for future authentication of the mobile user device. Applicant submits that "authentication" as claimed is distinct from the encryption system described by Hollis. With authentication the verifier is able to determine whether the mobile user device is who he says he is. By contrast, in encryption a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, Hollis fails to disclose the claimed authentication method.

Additionally, Hollis does not generate the public-private key pair on a mobile user device as claimed. As discussed above, in Hollis it appears that a centralized key authority (KA) is responsible for creation and distribution of public-private key pairs to rendezvous points (RVP). Such centralized key management and distribution system is distinct from the claimed

distributive system where each mobile device generates its own public-private key pair. Consequently, Hollis also fails to teach this limitation.

Claims 29, 30, 33, 34, 36, 37, 40, 41, 43, 44, 47, and 48

The Office Action rejected independent claims 29, 30, 33, 34, 36, 37, 40, 41, 43, 44, 47, and 48 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 7,162,037 to Joerg Schwenk (hereinafter "Schwenk").

The rejection is respectfully traversed in its entirety.

Schwenk describes a method for generating and regenerating an encryption key. In particular, Schwenk discloses an algorithm for allowing a user to reconstruct an encryption key by storing regeneration information at a trusted center. Consequently, Schwenk is focused on "encryption" keys. (See Col. 2, lines 28-67).

The present claims are focused on "authentication" of subscriber user device (e.g., mobile phones) with a network verifier. To clarify the focus of the present claims 29, 33, 36, 40, 41, 43, and 47, have been amended to recite that the public-private key pairs are generated and/or sent by a mobile user device (e.g., wireless phone, mobile phone, token, etc.) and used to authenticate the mobile user device.

Applicant submits that Schwenk fails to teach a method "operational in a mobile user device for authentication in a public cryptographic system ..." or a verification method/device configured to "receiving a first public key from a mobile user device, means for receiving a second public key from the mobile user device ..." As noted above, Schwenk is aimed at securing

By contrast, the present claimed invention is aimed at authenticating mobile user devices with a network verifier. Each mobile user device generates is own public-private key pair (and a backup public-private key pair) and distributes the public key to the verifier for future authentication of the mobile user device. Applicant submits that "authentication" as claimed is distinct from the encryption system described by Schwenk. With authentication the verifier is able to determine whether the mobile user device is who he says he is. By contrast, in encryption a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, Schwenk fails to disclose the claimed authentication method.

Additionally, Schwenk does not disclose generating the public-private key pair on a mobile user device as claimed. Therefore, Schwenk fails to anticipate this limitation.

Claim Rejections – 35 USC § 103

Claims 2-10, 15-18, and 23-25

The Office Action rejected claims 2-10, 15-18, and 23-25 under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 6,959,393 (hereinafter "Hollis") in view of Bruce Schneier's Applied Cryptography (hereinafter "Schneier").

The Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art references must teach or suggest all the claim limitations. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Third,

there must be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.

Claimed Elements are Not Taught or Suggested by the Prior Art

Applicant submits that neither Hollis nor Schneier teach the claimed limitations occurring in a system where mobiles user devices are authenticated by a network verifier device. In particular, the cited references fail to teach or suggest that mobile user devices generate and distribute their own public-private key pairs. For instance, Hollis appears to use a centralized key authority (KA) to generate and distribute its keys. Therefore, the claimed authentication system is a completely distinct system architecture than disclosed by the prior art. Consequently, prima facie obviousness has not been established as to these claims.

Based on at least the foregoing reasons, Applicant respectfully submits that independent claims 1, 11, 14, 19, 22, 26, 50 and 51 are patentably distinguishable over Hollis and independent claims 29, 33, 36, 40, 43, and 47 are patentably distinguishable over Schwenk. In view of the above, therefore, Applicant respectfully requests reconsideration and withdrawal of the rejection of, and/or objection and allowance of claims 1-51.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Applicant requests a **two month** extension of time in which to respond to the Office Action dated April 24, 2007. Please charge extension any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Date: September 24, 2007

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502